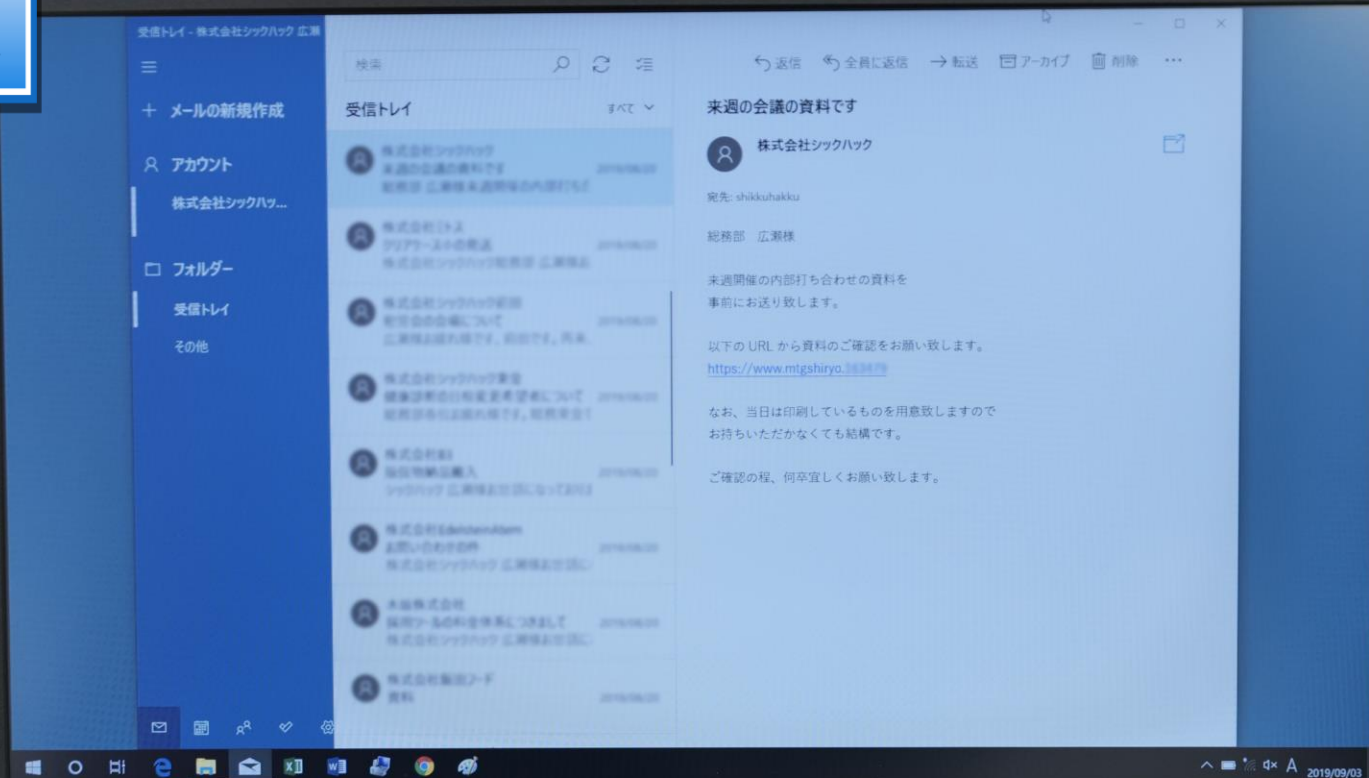


導入



今も、標的型攻撃の手口として一番よく使われているのが、メールを使った手口です。

導入



届いたメールの内容が、どこか心当たりがあると感じてしまうと、添付ファイルを開いたり、本文中にあるリンク先URLをクリックしたりして、つい確認をしてしまいがちですが、これが攻撃者の思うつぼとなってしまうのです。

導入



もしこんなメールが届いたら、皆さんはどう対処しますか？

事例

はいはい、
また仕事のメールでしょうね。

事例

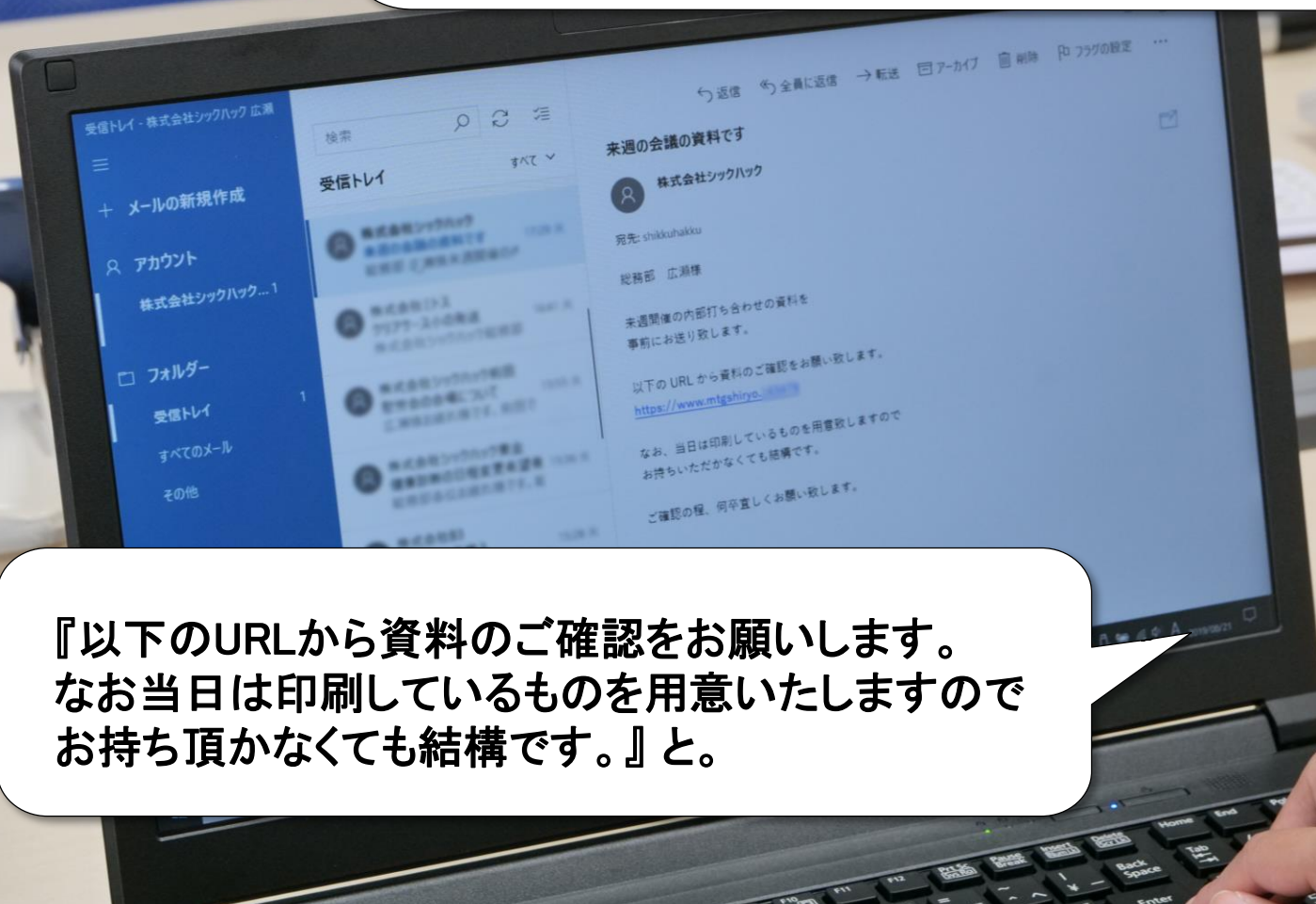
ん？なんだろう・・・
またセキュリティ更新かな？



事例

なになに、
『広瀬様、来週開催の内部打ち合わせの資料を事前に送ります。』
ですって？

『以下のURLから資料のご確認をお願いします。
なお当日は印刷しているものを用意いたしますので
お持ち頂かなくても結構です。』と。



事例

ふーん、
打ち合わせなんてあったかしら…

でも私の名前もちゃんと入っているし、一応確認しておこうかしら。

事例

あれ？

なになに、『これは訓練メールです』ですって？



事例

広瀬さん、どうかした！？

あっ田端さん、
メールのURLをクリックしたらこんな画面が表示されて……。



事 例

ああ、訓練メールをクリックしたのか。



事例

何か怪しいとは思わなかったのかな？

来週の内部打ち合わせって何かと思ったんですが、
自分の苗字が入っていたんで確認の為にクリックしました。

事 例

それがこのメール、
標的型攻撃メールの手口だよ。

自分の姓名が入っていて、内部資料とか書かれていると
怪しく見えなくなるだろ？

事例

はい、そうですね。
打ち合わせなんてあったかな？くらいしか
考えませんでした。

そうか、でもそのあったかな？という
違和感を感じる事が大事なんだ。

事例

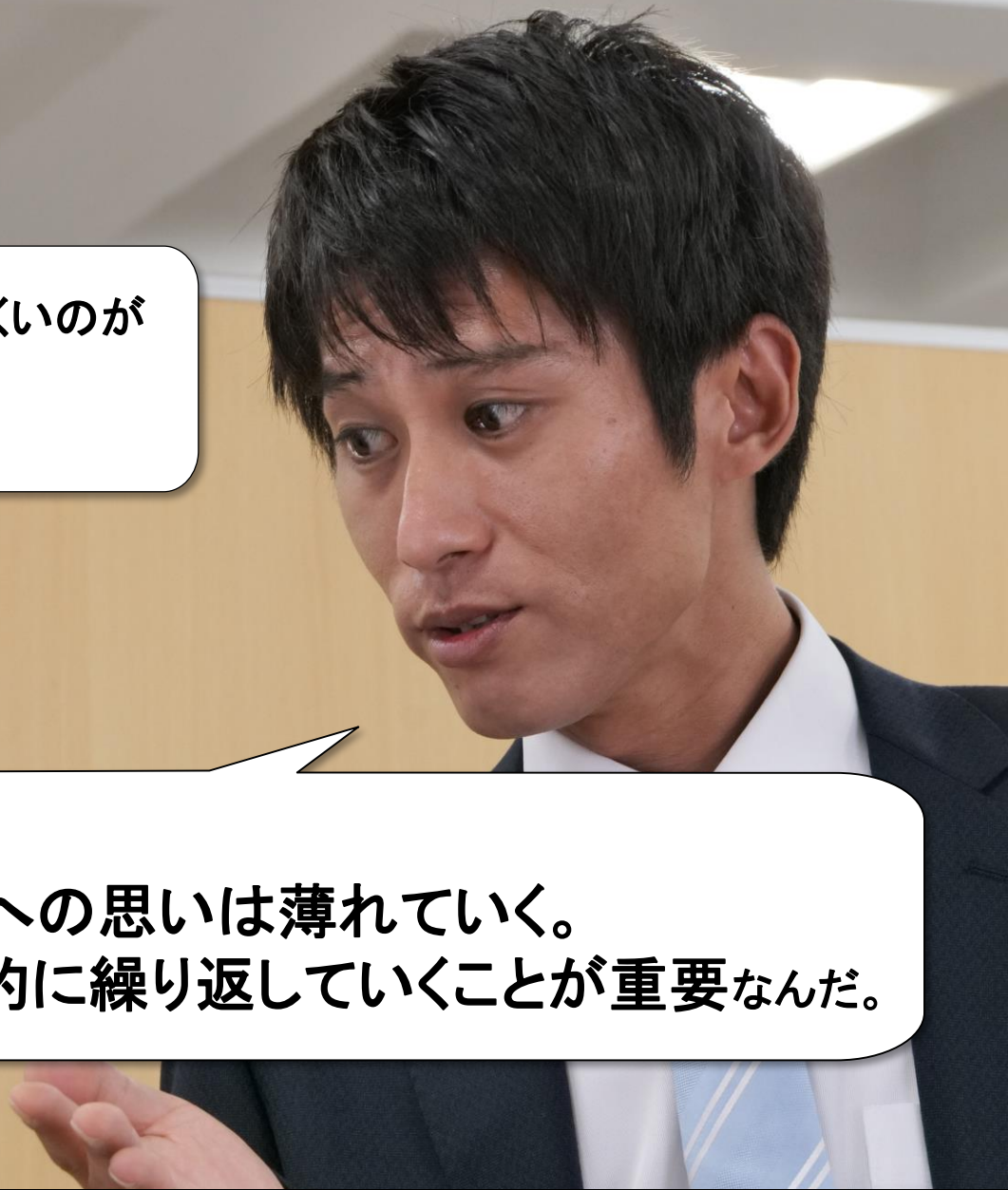
広瀬さんがこうしたメールにもう少し注意を払っていたら、URLをクリックする前に、私に打ち合わせがあるかを尋ねてきたと思うよ。

たしかにそうだったかも知れません。

事例

でも、怪しいメールとの区別が付きにくいのがこの攻撃の特徴でもあるから。そんなに落ち込まなくていいよ。

メールの利用は毎日のことだから、いくら注意していてもこうしたリスクへの思いは薄れていく。だからこの様な訓練を定期的に繰り返していくことが重要なんだ。



事例

わかりました。
少しでも怪しいと思うメールがあれば、
まずは報告ですね。

そういうことだ。



学習の意図



自分には思い当たらないと思うメールでも、自分の名前が入っているとつい確認したくなると思いますが、これが標的型攻撃メールの手口です。しかし、標的型攻撃メールかどうかを見分けることは、そう容易ではありません。

学習の意図



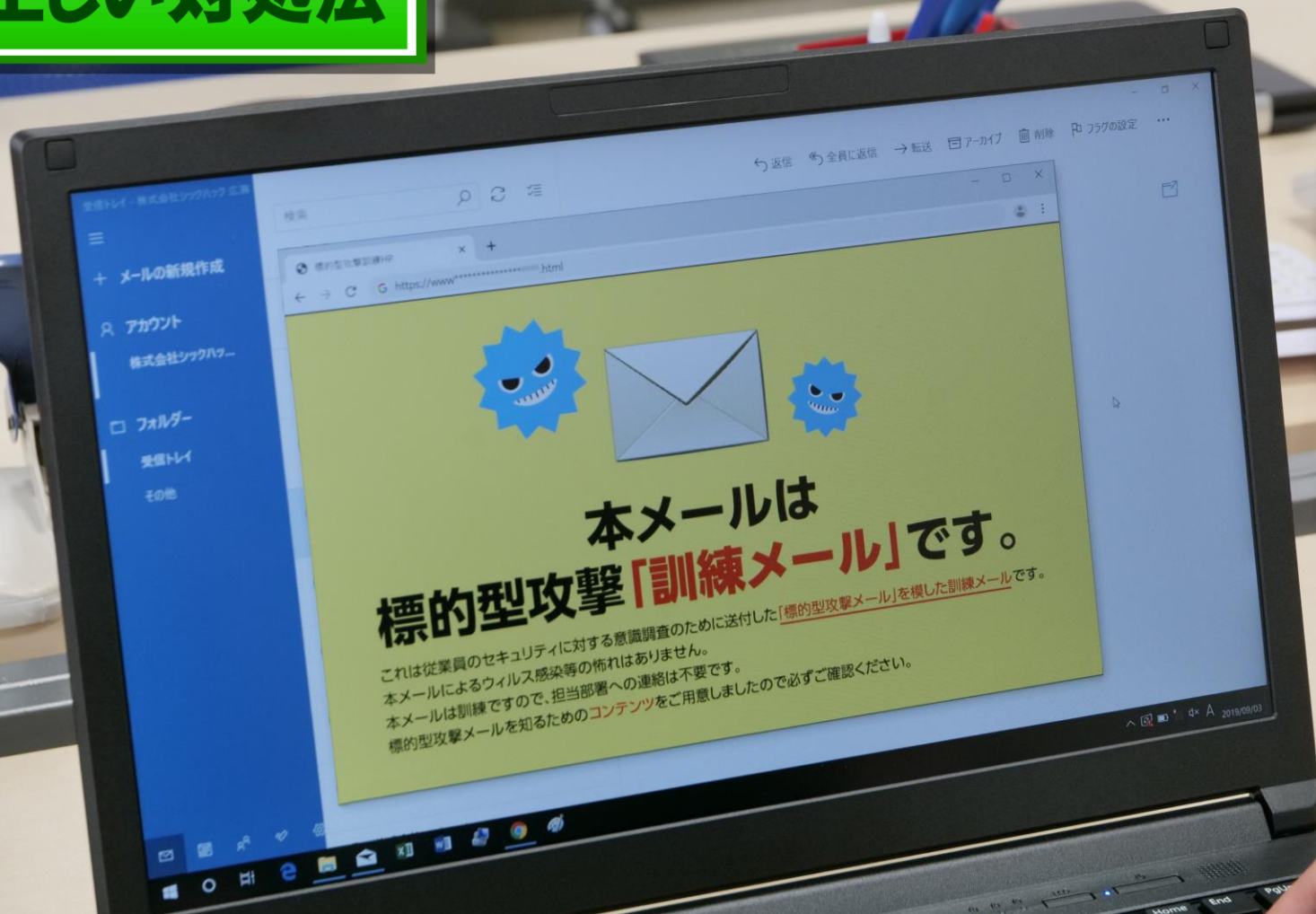
業務上、自分の知らない人からのメールを受け取ることもあるでしょう。しかし、そういう時でも、メールアドレスや本文内、添付ファイルに何か怪しい箇所がないか、注意深く確認をしましょう。一人では判断が付き難いのであれば、複数人に確認してもらいましょう。また、上司やシステム管理者にもその旨の報告を忘れずに行ないましょう。

学習の意図

「メール」について、以下を学習しましょう。

1. 少しでも怪しいと思うメールの添付ファイルや、
本文に書かれているリンク先URLはクリックしない
2. 不審メールについて、社内で情報の共有をしておく

正しい対処法



標的型攻撃メールなどの、いわゆる不審メールと判断した場合は、メールの添付ファイルを開いたり、本文に書かれているリンク先URLをクリックしたりしてはいけません。そもそも何ら問題のないメールでも、いきなり添付ファイルやリンク先URLを開いたりクリックしたりする行為は行うべきではありません。

正しい対処法

標的型攻撃メールと言っても、不特定多数にばらまかれる場合もあり、他の部署にも同じようなメールが届いている可能性もあります。こうしたメールの情報は、上司やシステム管理者に報告して社内で共有しておくことで、今後同じようなメールが届いた場合に適切な対応が行えるでしょう。